Web Images Videos Maps News Shopping Gmail more ▼

Sign in

Google scholar digital signature conjugacy search problem Search Advanced Scholar Search Scholar Preferences

Scholar Articles and patents anytime include citations Results **1** - **10** of about **18,700. (0.18** sec)

New public-key cryptosystem using braid groups psu.edu [PDF]

KH Ko, SJ Lee, JH Cheon, JW Han, J Kang, C ... - Lecture Notes in ..., 2000 - Springer

... hard **problems** in combinatorial group theory such as the word **problem** [1,37,17] or using the Lyndon words [31]. Recently Anshel- Anshel-Goldfeld proposed in [2] a key agreement system and a PKC using groups where the word **problem** is easy but the **conjugacy problem** is ...

Cited by 184 - Related articles - BL Direct - All 18 versions

[PDF] New **signature** scheme using **conjugacy problem** psu.edu [PDF]

KH Ko, DH Choi, MS Cho, JW Lee - preprint, 2002 - Citeseer

... More precisely the schemes are based on the **conjugacy** Diffie-Hellman **problem**. ... This difficulty has been hampering a proposal of a **signature** scheme on non-commutative algebraic structure. In this paper we propose a new **digital signature** scheme based on a variation of the ...

Cited by 38 - Related articles - View as HTML - All 6 versions

Group **signature** schemes using braid groups arxiv.org [PDF]

T Thomas, AK Lal - Arxiv preprint cs/0602063, 2006 - arxiv.org

... Group **signatures** can also be integrated with an electronic cash system whereby several banks can securely distribute anonymous ... 2.5 Hard **Problems** in Braid Groups We use the following hard **problems** in our **signature** schemes. 1. **Conjugacy Search Problem** (CSP) ...

Cited by 10 - Related articles - View as HTML - All 3 versions

One **digital signature** scheme in semimodule over semiring mii.lt [PDF]

E Sakalauskas - Informatica, 2005 - IOS Press

... Soc., 79(3), 569–604. Goldwasser, S., S. Micali, R. Rivest (1988). A **digital signature** scheme secure against adaptive chosen message attacks. ... Ki Hyoung, Ko, Doo Ho Choi, Mi Sung Cho, Jang Won Lee (2002). New **Signature** Scheme Using **Conjugacy Problem**. ...

Cited by 8 - Related articles - All 5 versions

[PDF] Blind **signature** scheme over braid groups iacr.org [PDF]

GK Verma - Preprint, http://eprint. iacr. org/2008/027, 2008 - eprint.iacr.org

... Blind **signatures** are the basic tools of **digital** cash payment systems, electronic voting systems ...

In this paper we have proposed two blind **signature** schemes over Braid groups. ... public key cryptosystem on braid groups based on the difficulty of solving **conjugacy search problem**. ...
Cited by 5 - Related articles - View as HTML - All 2 versions

A technique for image encryption using **digital signature** 202.127.1.11 [PDF]
A Sinha, K Singh - Optics Communications, 2003 - Elsevier
... tips (Opens new window) Journal/book title. Volume Issue Page Clear all fields Advanced **Search**. ... been used [6] to decrypt the encoded image instead of using the complex **conjugate** of the ... Since the size of the **digital signature** is fixed, error control codes of different strengths are ...
Cited by 31 - Related articles - All 6 versions

Key agreement protocol (KAP) using **conjugacy** and discrete logarithm **problems** in ... mii.lt [PDF]
E Sakalauskas, P Tvarijonas, A Raulynaitis - Informatica, 2007 - IOS Press
... Page 9. Key Agreement Protocol (KAP) Using **Conjugacy** and Discrete Logarithm **Problems** 123 ... Sakalauskas, E. (2005). One **digital signature** scheme in semimodule over semiring. ... The **conjugacy search problem** in public key cryptography: unnecessary and insufficient. ...
Cited by 7 - Related articles - All 5 versions

[PDF] Post-quantum **signatures** psu.edu [PDF]
J Buchmann, C Coronado, M Döring, D Engelbert, C ... - Preprint, 2004 - Citeseer
... So Shor's algorithm breaks all **digital signature** schemes in use today. ... The **signature** variant of that system is described in Section 5.1. ... The **Conjugacy Search Problem** (CSP) and its variations are the starting point for the construction of one-way functions. ...
Cited by 5 - Related articles - View as HTML - All 11 versions

[PDF] A proxy **signature** scheme over braid groups iacr.org [PDF]
GK Verma - 2008-05-18], http://eprint, iaer. org/2008/160, pdf - eprint.iacr.org
... Several other **digital signature** schemes have also been proposed but no proxy **signature** scheme has ... the following features and implications: - This is a first proxy **signature** scheme over ... of the Braid groups and discuss some hard **problems** related to **conjugacy search problem**. ...
Cited by 3 - Related articles - View as HTML - All 2 versions

[PDF] Designated verifier **signature** scheme based on braid groups psu.edu [PDF]
Z Shi-hua, Z Ji-wen, Q Jun-jie - 2008-05-18]. http://eprint. iacr. org/2006/329. pdf - Citeseer
... in 2001 [4], **digital signature** schemes by Ko et al.in2002 [5],an entity authentication scheme by Sibert et al.in 2002 ... 1 ,π 2 ,...,π p) which can be processed by the computer. We use the following hard **problems** in our **signature** scheme: 1 **Conjugacy Search Problem** (CSP) ...
Cited by 4 - Related articles - View as HTML - All 4 versions

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

digital signature conjugacy search p Search

Go to Google Home - About Google - About Google Scholar